PERIODICO MARITTIMO INDIPENDENTE A DIFFUSIONE INTERNAZIONALE
A BILINGUAL SHIPPING NEWSPAPER
L'INFORMATORE NAVALE
FONDATO NEL 1964 di NAPOLI

OCEANLY – MINACCIA CYBER: ALLARME SU PORTI, NAVI E LOGISTICA

Gian Enzo Duci: "Investire in sistemi anti-hacker per difendere e accelerare la digitalizzazione in atto"

"Si delinea con sempre maggiore chiarezza un paradosso: nel momento in cui l'industria del mare accelera verso una digitalizzazione e sistemi di automazione in grado di migliorare l'efficienza, ridurre i consumi e le emissioni, la minaccia dei cyber attack costringe anche il mondo dello shipping, e più in generale quello dei trasporti, a tirare il freno a mano"

La denuncia è di Gian Enzo Duci, managing director di Oceanly, la società genovese che in pochi mesi ha conquistato la leadership a livello mondiale nel monitoraggio a distanza delle performance delle navi gasiere LNG e che è ora in grado di fornire alle principali compagnie di navigazione e di ship-management.

"*Come gruppo* – prosegue Duci, impegnato in una ricerca di lungo termine sul fenomeno cyber e i contraccolpi nel settore shipping e logistica – *abbiamo sviluppato un sistema che consente di monitorare in remoto tutte le performance della nave, contenere i consumi, ridurre drasticamente le emissioni, programmare la manutenzione della nave, suggerire persino i cambiamenti di rotta che consentono di ottimizzare l'utilizzo dei motori. Ma ci troviamo di fronte a una devils alternative: da un lato il processo di digitalizzazione del trasporto, e in particolare di quello marittimo, non deve subire rallentamenti; dall'altro, proprio la digitalizzazione (specie quella ormai un po' datata e non accompagnata da sistemi di difesa e protezione) espone porti, navi e catena logistica a rischi potenzialmente devastanti".*

I numeri sono impietosi: secondo il World Shipping Council per scoprire di essere oggetto di un hackeraggio in corso per un operatore marittimo trascorrono dai 100 ai 140 giorni. Molto spesso i sistemi di digitalizzazione obsoleti che ancora caratterizzano una percentuale consistente della flotta mondiale, sono la porta d'ingresso preferita per attacchi che, nel caso di navi passeggeri, può tradursi nel furto di una massa enorme di dati sensibili e su tutte le navi nel potenziale controllo dei sistemi di bordo (non è un caso che smentire un eventuale attacco cyber sia stata una delle prime preoccupazioni delle Autorità coinvolte nell'analisi del tragico abbattimento, da parte della portacontainer Dali, del Francis Scott Bay Bridge). Anche a terra la situazione non è migliore: nei porti un blackout, attraverso la penetrazione del PCS, può interrompere l'interfaccia fra nave e terminal; nella catena logistica,

infine, una disconnessione fra i flussi informativo-documentali e i flussi di merce sarebbe oggi sufficiente ad affermare il caos.

"È cosa nota - prosegue Duci - *che gran parte degli attacchi cyber fatti a fini estorsivi non venga denunciata e che le vittime preferiscano negoziare, attraverso soggetti internazionali specializzati, con gli hackers per ottenere la restituzione dei dati sensibili. Ma in uno scenario di instabilità come quello in cui viviamo, gli attacchi cyber si potrebbero trasformare in veri e propri atti di terrorismo o ancor peggio di guerra".*

"In un porto un attacco cyber anche solo ai sistemi e alle gru di movimentazione delle merci - conclude Duci - *può avere gli effetti di un vero e proprio bombardamento. E una volta superata la "contraerea" dei sistemi di protezione, è sempre più difficile mettere in essere un piano B: più il processo di digitalizzazione è spinto, meno possibilità si hanno di un ritorno, anche temporaneo, alla gestione material-manuale, con il rischio che le tempistiche di restore diventino il freno della rivoluzione digitale.*